Abusing RFID for fun & profit.

Youri ”iTdeal” van der Zwart
Jurre ”DrWhax” van Bergen

Introduction

$whoarewe

Outline

- What is RFID?
- Failed implementations.
  - Ov-Chipcard
  - Metapay
  - University cards
- MijnID

What is RFID

- Radio-Frequency-Identification
- Works on various frequencies
- Broad usages
- Used around the world

Usages

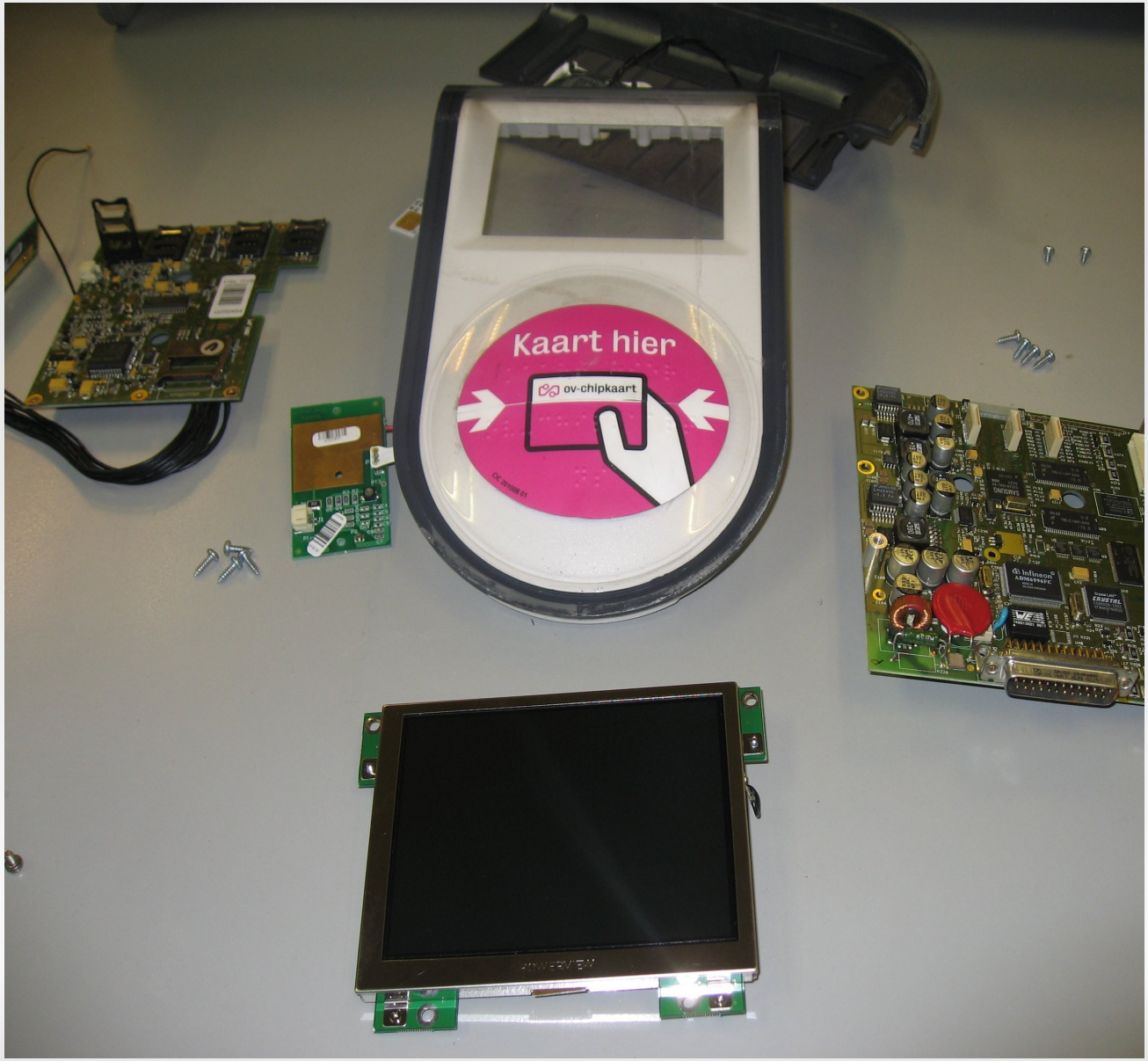
- Hotels (13,56mhz, NL)
- Public transport (13,56mhz, NL)
- Passport (900mhz .NL)
- Credit cards (900mhz?)

Failed implementations

Ov-chipkaart

- Mifare cards
- Mifare Classic proven to be insecure '08
- Backoffice system mapped.

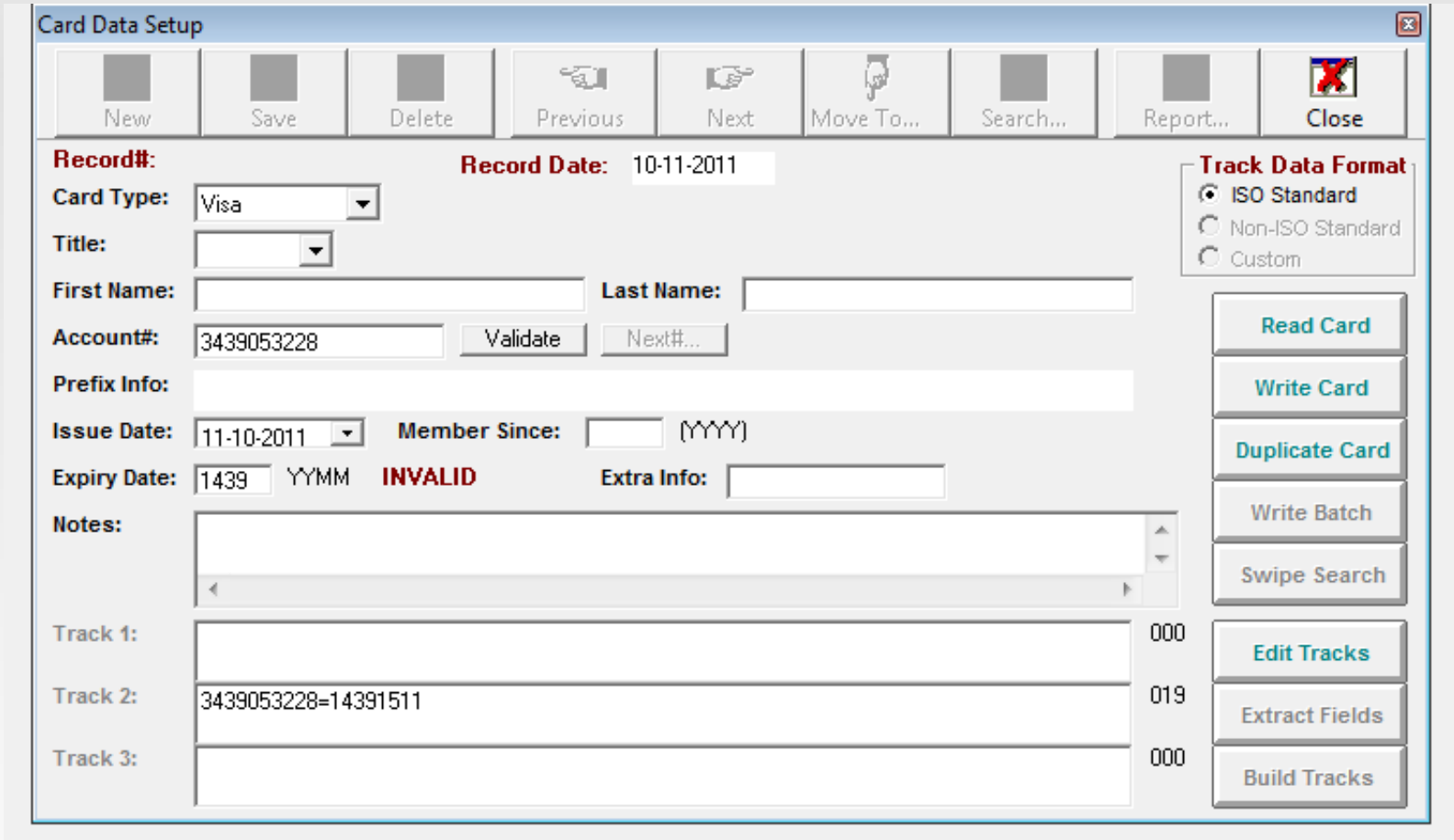
Hardware



Ov-chipkaart metro system

- No encryption at all \o/
- One write only.
- Being used for one way/round trip.
- Hardware created to bruteforce UID's.

Magnetic swipe side



Adam University card

Metapay

The card is an RFID card using near field communication technology.

The card is not deemed a bank card or a payment instrument substituting cash and Sziget does not hold deposits. It may only be used for payment at the Budai Gourmet, the Volt Festival, the Heineken Balaton Sound and Sziget events, during the event, in the sales units operating at the premises of the event provided by Sziget. The balance of the voucher purchased is not stored on the card. The festival card is valid at each of the above events, but the balance on the card may NOT be transferred to another of the above events. The balance on the card may be reimbursed. For the rules of reimbursement, see Point 8.

The card does not make it possible to personally identify the cardholder and it carries no information regarding its holder.

0day time!

- AH mijnid
- Mifare ultralight
- UID coupled to your back account
- Self service
- Bruteforcing for free 0xf00d.

DIY

Come tonight to the hackerspaces village!

RFIDIOT, mfoc, touchatag

Thanks for listening!

DrWhax

iTdeal